REMARKS/ARGUMENTS

Claims 1-2, 10, 12-14, and 20 stand rejected under 35 U.S.C. 102(e) as being anticipated by United States Patent Application Publication No. 2002/0093567 by Cromer et al. ("Cromer"). In addition, Claims 3-4 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer in view of United States Patent Application Publication No. 2003/0196114 by Brew et al. ("Brew"). In addition, Claims 7-9, 11, and 15-17 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer in view of United States Patent No. 5,670,984 to Robertson et al. ("Robertson"). Finally, Claims 5-6 and 18-19 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer in view of Brew and United States Patent Application Publication No. 2002/0087894 by Foley et al. ("Foley").

The Applicant notes that Cromer is a new reference not cited by the Examiner in the previous Office Actions. The Applicant also notes that the Examiner has dropped his citation of United States Patent No. 5,638,523 to Mullet et al. ("Mullet").

The Examiner is respectfully requested to consider the original and previously presented claims in view of the following comments.

Claim 1:

For reference, original Claim 1 recites the following:

> 1. (Original) A method for controlling access to secured information for a predetermined region of a computer generated original image presented on a display, comprising:
>
> determining whether a user is authorized to access said secured information; and,
>
> in response to said determining, distorting said original image to produce a distorted region for said predetermined region to provide said user with said secured information on said display.

On pages 2-3 of the Office Action the Examiner cites Cromer against Claim 1 stating (underling added):

> "As to claim 1, Cromer discloses a method for controlling access to secured information for a predetermined region of a computer generated original image presented on a display (abstract), comprising:...determining whether a user is authorized to access said secured information ([0034]); and, in response to said determining, distorting said original image to produce a distorted region for said predetermined region to provide said user with said secured information on said display ([0032], [0034], see also [0011], [0031], lines 14-19)."

For reference, the selections from Cromer cited by the Examiner above recite the following (underlining added):

> "**Abstract**...A method and system are disclosed for generating and distributing a digital photographic proof. An altered image is generated by altering original image data to produce altered image data. The altered image data is stored in an electronic file. The encrypted instructions are stored in the file with the altered image data. The instructions describe a method for reversing an alteration method utilized to alter the original image to produce the altered image data. A digital photographic proof is produced utilizing the file by displaying the altered image. All users are permitted to view the altered image. Only authorized users are permitted to utilize the encrypted instructions to reproduce the original image from the altered image data. Only authorized users may reproduce the original image. The single electronic file is thus utilized to both produce a digital photographic proof and to reproduce the original image."

> "SUMMARY OF THE INVENTION...**[0011]** A method and system are disclosed for generating and distributing a digital photographic proof. An altered image is generated by altering original image data to produce altered image data. The altered image data is stored in an electronic file. The encrypted instructions are stored in the file with the altered image data. The instructions describe a method for reversing an alteration method utilized to alter the original image to produce the altered image data. A digital photographic proof is

produced utilizing the file by displaying the altered image. All users are permitted to view the altered image. Only authorized users are permitted to utilize the encrypted instructions to reproduce the original image from the altered image data. Only authorized users may reproduce the original image. The single electronic file is utilized to both produce a digital photographic proof and to reproduce the original image."

"**[0031]** FIG. 3 depicts a high level flow chart which illustrates an authorized user, such as the owner of the original image, embedding a method in an altered image describing how to reverse the alteration method used to alter the image in accordance with the method and system of the present invention. The process starts as depicted at block **300** and thereafter passes to block **302** which illustrates capturing a visual image utilizing a digital camera. When a visual image is captured, the digital camera will generate digital data which represents the image. The original, unaltered data which represents the original image is stored in the digital camera. Next, block **304** depicts removing either the data which represents the image or a copy of the data from the camera. For example, the image data may be transmitted from the camera to computer system **12**. Thereafter, block **306** illustrates selecting an alteration method to use to alter the image data. Many alteration methods are currently known. The color of the original image may be distorted in some manner. Or, for example, the word 'PROOF' might be inserted into the digitized image."

"**[0032]** Block **308** depicts the alteration of the original image data using the alteration method selected as illustrated by block **306**. Thereafter, block **310** depicts the creation of instructions which describe the method necessary to reverse the alteration of the image data. Any user who has access to the instructions will be able to reproduce the original, unaltered image by following the instructions. The process then passes to block **312** which illustrates encrypting the instructions utilizing any known encryption method. In a preferred embodiment, the instructions will be encrypted using industry standard methods such as RSA public/private key. Then, block **314** depicts appending the encrypted instructions to the altered image data. Thereafter, block **316** illustrates storing the altered image data along with the encrypted instructions together in a single electronic file. The process then terminates as depicted by block **318**."

"**[0034]** Next, block **406** illustrates a determination of whether or not the user has purchased the right to reproduce the original image in its unaltered form. If a determination is made that the user has not purchased the right to reproduce the original image in its unaltered form, the process passes to block **408** which depicts the user being permitted to access only the altered image. The altered image data is utilized to produce the altered image. The process then terminates as illustrated by block **410**."

Also, please consider the following additional selections from Cromer (underling added):

"**[0005]** Photographers need the ability to provide a test print of an image to potential buyers without the fear that the test print will be misused. The test print is called a 'proof'. Traditionally, the photographer provided a proof to a potential buyer by developing a print from the negative and marking the print in a destructive manner by adding the word 'proof' to the photograph. Alternatively, a photographer might use photographic paper which indicated that the photograph was a proof and which included a copyright notice. Professional film developers typically respected the owner's rights in the photograph and refused to reproduce proofs. Further, it is difficult to completely remove a 'proof' symbol from a traditional photograph. Therefore, using conventional cameras and film developing techniques, it is difficult to make a high quality reproduction of a photographic proof."

"**[0006]** If after viewing the proof the potential buyer decided to purchase the photograph, the photographer could make a high quality reproduction by producing another photograph from the negative without adding a 'proof' symbol. Therefore, with conventional analog cameras, a photographer could easily retain the means to produce the highest possible quality photographic print by retaining the negative of the image."

"**[0008]** Known systems have recognized this problem. One approach offered to solve this problem is to provide two separate images to a potential buyer. One image is a proof image which is a lower quality image and which is viewable by all users. The other image is a high quality image. The high quality image is encrypted so that it cannot be viewed or printed.

After the potential buyer has paid for the right to reproduce the high quality image, the owner of the image can provide a decryption key to decrypt the encrypted high quality image. The decryption key is provided and distributed electronically, for example using a floppy diskette, separately from the encrypted image."

"**[0009]** This solution requires that the photographer provide two separate images. One image is a proof and the other image is the encrypted original image. Further, the photographer must be contacted and must provide the decryption key when payment has been made."

"**[0019]** The present invention is a method and system for generating and distributing a digital photographic proof. An original image is captured utilizing a digital camera. The original image is represented by original image data which is stored either within the camera or made available to the photographer outside of the camera. The photographer may choose to generate and distribute a digital proof of the original image to potential buyers."

"**[0020]** The photographer may generate a digital proof by first choosing an alteration method to use to alter the original image data. Known systems for altering digital photographic data include modifying the image color, shaping random pixels, or modifying all or part of the image using an encryption key. The photographer will then alter the original image data using the chosen alteration method to create altered image data."

"**[0025]** When a potential buyer has purchased the right to reproduce the original image data, the photographer will provide the decryption key to the buyer. The buyer will then be able to use the decryption key to decrypt the instructions and reproduce the original image from the altered image data. In this manner, the original image is reproduced from the same file which produced the digital proof. Further, the file which was used to produce both the digital proof and to reproduce the original image includes instructions describing how to reproduce the original image from that file."

First: It would appear that Cromer describes a method that produces a result that is the opposite to that produced by Claim 1.

In particular, in Cromer, the user is first provided with a proof or altered image. The proof image is generated by altering an original image using an alternation method. If the user is granted access to the original image (i.e., by way of being provided with a decryption key), the original image is then generated from the proof image using instructions included in the file containing the proof image. The result is that the user is provided with the original image.

In contrast, in Claim 1, the user is first provided with the original image. If the user is granted access to secured information relating to a predetermined region of the original image, then the original image is distorted to produce a distorted region for the predetermined region. The distorted region provides the user with the secured information. The result is that the user is provided with a distorted image (i.e., an original image having a distorted region within it).

As such, Cromer does not teach or suggest the subject matter of Claim 1. In fact, it would appear to teach the opposite.

As such, Cromer does not teach or suggest those elements of Claim 1 that recite: "A method for controlling access to secured information for a predetermined region of a computer generated original image presented on a display…:" ; and, "in response to said determining, distorting said original image to produce a distorted region for said predetermined region to provide said user with said secured information on said display."

Second: In Cromer, the proof image provides the user with the information they need to make a decision as to whether or not they would like to buy the original image. The quality of the original image is what is altered by the proof image, not the content of the original image. The proof image does not hide content from the user. If it did, then users would not know whether to buy the original image or not.

In contrast, in Claim 1, content (i.e., "secured information") is hidden or withheld from the user when the user is presented with the original image. The secured information is only provided to the user then the original image is subsequently distorted.

As such, Cromer does not teach or suggest those elements of Claim 1 that recite: "A method for controlling access to secured information for a predetermined region of a computer generated original image presented on a display…;" ; and, "in response to said determining, distorting said original image to produce a distorted region for said predetermined region to provide said user with said secured information on said display."

Third: In paragraphs 0005 and 0020, Cromer provides examples of the alternations that may be applied to original image to produce a proof image. These include adding a proof symbol, "modifying the image color", "shaping random pixels", or "modifying all or part of the image using an encryption key". These alteration methods do not amount to adding a lens to the original image as is implied by the use of the expressions "distorting" and "distorted region" in Claim 1.

As such, Cromer does not teach or suggest that element of Claim 1 that recites: "in response to said determining, distorting said original image to produce a distorted region for said predetermined region to provide said user with said secured information on said display."

Summary:

In summary, the Applicant respectfully submits that Claim 1 is patentable over Cromer as this reference does not teach or suggest the subject matter of Claim 1. In addition, the Applicant submits that Claims 2-19, being dependent on Claim 1 and adding patentable features thereto, are also patentable.

For the reasons given above with respect to Claim 1, the Applicant respectfully submits that Claim 20 is patentable.

No new matter has been entered by the above noted amendments (if any).

The Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

McCarthy Tétrault LLP

Date: April 22, 2008

By: 

Joseph P. Conneely
Registration No. 54,883
Telephone: (416) 601-8179
Fax: (416) 868-0673

McCarthy Tétrault LLP
Box 48, Suite 5300
66 Wellington Street West
Toronto Dominion Bank Tower
Toronto, Ontario, Canada
M5K 1E6